Finite Fields and Their Applications 18 (2012) 210–221

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On the dual of the dual hyperoval from APN function $f(x) = x^3 + Tr(x^9)$

Hiroaki Taniguchi

Kagawa National College of Technology, 551 Takuma, Kagawa, 769-1192, Japan

ARTICLE INFO

Article history:
Received 24 February 2010
Revised 16 May 2011
Accepted 23 July 2011
Available online 30 August 2011
Communicated by Gary McGuire

MSC:
51A45
51E20
51E21

Keywords:
Dual hyperoval
Quadratic APN function

ABSTRACT

Using a quadratic APN function f on $GF(2^{d+1})$, Yoshiara (2009) [15] constructed a d-dimensional dual hyperoval S_f in $PG(2d+1,2)$. In Taniguchi and Yoshiara (2005) [13], we prove that the dual of S_f, which we denote by $S_f^{\perp}$, is also a d-dimensional dual hyperoval if and only if d is even. In this note, for a quadratic APN function $f(x) = x^3 + Tr(x^9)$ on $GF(2^{d+1})$ by Budaghyan, Carlet and Leander (2009) [2], we show that the dual $S_f^{\perp}$ and the transpose of the dual $S_f^{\perp T}$ are not isomorphic to the known bilinear dual hyperovals if d is even and $d \geqslant 6$.

1. Introduction

Let m and d be integers with $m > d \geqslant 2$. Let $PG(m,q)$ be an m-dimensional projective space over the finite field $GF(q)$ consisting of q-elements.

A family S of d-dimensional subspaces of $PG(m,q)$ is called a d-dimensional dual hyperoval in $PG(m,q)$ if it satisfies the following conditions:

(1) any two distinct members of S intersect in a projective point,
(2) any three mutually distinct members of S intersect trivially,
(3) the union of the members of S generates $PG(m,q)$, and
(4) there are exactly $q^d + q^{d-1} + \cdots + q + 2$ members of S.

E-mail address: taniguchi@dg.kagawa-nct.ac.jp.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2011.07.009

The definition of higher dimensional dual hyperovals was first given by C. Huybrechts and A. Pasini in [7]. We refer to the space $PG(m,q)$ of (3) above as the ambient space of the dual hyperoval S. For d-dimensional dual hyperovals S_1 and S_2 in $PG(m,q)$, we say that S_1 is isomorphic to S_2 by the mapping Φ, if Φ is a linear automorphism of $PG(m,q)$ which sends the members of S_1 onto the members of S_2. If $S_1 = S_2 := S$, we say that Φ is an automorphism of S.

The 2-dimensional dual hyperovals over $GF(2)$ have been classified by Del Fra [3]. In this article, we assume that $q = 2$ and $d \geqslant 3$.

Let $K := GF(2^{d+1})$. Let $K^\times$ be the multiplicative group of K. Let us define a multiplication $K \times K \ni (x,y) \mapsto x * y \in K$ which satisfies the right and left distributive law. We assume that the multiplication $*$ also satisfies the following conditions (i) and (ii):

(i) for any $t \in K^\times$, there exists a unique $x \in K^\times$ such that $x * t = 0$, and
(ii) for any $x \in K^\times$, there exists a unique $t \in K^\times$ such that $x * t = 0$.

These conditions (i) and (ii) are not equivalent. In fact, for $x * t := x^\sigma t + xt^\tau$ where σ and τ are elements in the Galois group $Gal(K/GF(2))$ of K over $GF(2)$, (i) implies that σ is a generator of $Gal(K/GF(2))$, and (ii) implies that τ is a generator.

Let ϕ be the one-to-one mapping from K to itself such that $\phi(0) = 0$ and $\phi(t) * t = 0$ for all $t \in K$. Property (i) guaranties that ϕ is a function and property (ii) that it is a bijection.

Let $S := \{X(t) \mid t \in K\}$ be a set of d-subspaces in $PG(2d+1,2) = (K \times K)\backslash\{(0,0)\}$, where $X(t) := \{(x, x*t) \mid x \in K^\times\} \subset (K \times K)\backslash\{(0,0)\}$. Since the multiplication $*$ satisfies (i), for any distinct $s, t \in K^\times$, the intersection $X(s) \cap X(t)$ is a unique projective point:

$$X(s) \cap X(t) = \big(\phi(s+t), \phi(s+t) * s\big) = \big(\phi(s+t), \phi(s+t) * t\big).$$

Since the multiplication $*$ satisfies (ii), no three mutually distinct members of S have a common point. Since the cardinality $|S| = |K| = 2^{d+1}$, we see that S is a d-dimensional dual hyperoval inside $PG(2d+1,2)$. Moreover, S has the translation automorphisms t_a for any $a \in K$ defined by $t_a : K \times K \ni (x,y) \mapsto (x, y + x*a) \in K \times K$, which send $X(t)$ to $X(t+a)$ for any $t \in K$, since t_a maps any member $(x, x*t)$ of $X(t)$ to a member $(x, x*t + x*a) = (x, x*(t+a))$ of $X(t+a)$.

We refer to the dual hyperoval S as a **bilinear dual hyperoval**, since $x*t$ is $GF(2)$-bilinear function on x and t. The above construction of a bilinear dual hyperoval is an analogy of the construction of a spread set from a semifield. Note that there are non-bilinear d-dimensional dual hyperovals in $PG(2d+1,2)$. See [10,11,13]. Recently, Edel studied on the representations of bilinear dual hyperovals in Section 5 of [5].

We recall Knuth's S_3 (the symmetric group of order 6) on semifields, which is generated by two involutional operations: One reverses the order of multiplication ($y * x$ instead of $x * y$), the other replaces the spread sets by their duals under the symplectic bilinear form. So, he defined the transpose π^T and the dual π^D for the semifield plane π in [8], and studied on six members π, π^T, π^D, π^{TD}, π^{DT} and π^{TDT}. (Also see [1].)

As an analogy of Knuth's S_3, we define the transpose S^T and the dual $S^\perp$ for a bilinear dual hyperoval S as follows: We define the transpose of S as $S^T := \{X^T(t) \mid t \in K\}$, where $X^T(t) := \{(x, t*x) \mid x \in K^\times\}$. Let Tr be the trace function from K to $GF(2)$. We define the dual of S under the non-degenerate symplectic bilinear form $(K \times K) \times (K \times K) \ni ((s,y),(x,t)) \mapsto Tr(yx + st) \in GF(2)$ as $S^\perp := \{X^\perp(t) \mid t \in K\}$, where $X^\perp(t) := \{(s,y) \mid Tr(yx + s(x*t)) = 0 \text{ for any } x \in K\}$. Unfortunately, $S^\perp$ is not always a dual hyperoval. (See Theorem 1.) However, if $S^\perp$ is a dual hyperoval, then $S^\perp$ is also a bilinear dual hyperoval. (See Proposition 7 of [5].) On the other hand, S^T is always a bilinear dual hyperoval.

Now, we are able to consider the six members S, S^T, $S^\perp$, $S^{T\perp}$, $S^{\perp T}$ and $S^{T\perp T}$. We also think that the method of cubical array in [8] will be useful on the study of bilinear dual hyperovals. The cubical array $\{C_{i,j,k}\}$ is just a representation of the $GF(2)$-bilinear mapping $x*t$ with respect to some chosen basis $\{e_0, e_1, \ldots, e_d\}$, that is, $\sum_k C_{i,j,k} e_k = e_i * e_j$. By permuting the roles of the indices of $\{C_{i,j,k}\}$, we get the $GF(2)$-bilinear mappings that generate S^T, $S^\perp$, etc. However, we will not go further on the relation between bilinear dual hyperovals and the cubical arrays in this paper.

We also recall that, we have a semibiplane from the dual hyperovals [16], which is an analogy of the Andre–Bruck–Bose construction of the semifield plane from the spread.

By now, any known bilinear dual hyperoval belongs to the following two families. The first family consists of the bilinear dual hyperovals with $x * t := x^\sigma t + xt^\tau$, where σ and τ are generators of $Gal(K/GF(2))$ with $\sigma\tau \neq id$. This family is studied by Yoshiara in [14]. We refer to the member of this family as a **Yoshiara's bilinear dual hyperoval.**

We call a function f on K Almost Perfect Nonlinear (APN) if, for every $a \neq 0$ and every b in K, the equation $f(x+a)+f(x)=b$ admits at most two solutions. We also call f on K as quadratic if $f(x+t)+f(x)+f(t)+f(0)$ is $GF(2)$-bilinear on x and t. Two functions f and g on K are extended affine equivalent if, there exist affine permutations A_1 and A_2 and an affine mapping A on K such that $f(x) = A_2(g(A_1(x))) + A(x)$ for any x in K.

In the second family of bilinear dual hyperovals, $x * t$ is defined as $x * t := f(x+t) + f(x) + f(t) + f(0)$, where f is a quadratic APN function. This construction was also discovered by Yoshiara in [15]. We note that, in the second family, $x * t$ is an alternating mapping on x and t, that is, $t * t = 0$ for any $t \in K$ (hence we have $x * t = t * x$). For several geometric approaches to APN functions other than dual hyperovals, see [9].

In Theorem 2, we present bilinear dual hyperovals which do not belong to the above families.

In this paper, since we have to distinguish several types of bilinear mappings $x * t$, from now on, we denote this bilinear map by $B(x,t)$ instead of $x * t$, and the corresponding dual hyperoval by S_B instead of S. Also, we write by ϕ_B instead of ϕ. If B is an alternating mapping, we write by $A(x,t)$ for $B(x,t)$, and by $A_f(x,t)$ if the alternating mapping A is from a quadratic APN function f, that is, if $A(x,t) = f(x+t)+f(x)+f(t)+f(0)$. We call S_A an **alternating bilinear dual hyperoval**, and S_{A_f} an **APN dual hyperoval**.

Edel proved in Theorem 1 of [4] that S_A is isomorphic to S_{A_f} for some quadratic APN function f. Moreover, he proved in Theorem 1 of [4] that, for quadratic APN functions f and g, dual hyperovals S_{A_f} and S_{A_g} are isomorphic if and only if f and g are extended affine equivalent.

If S_B is a bilinear dual hyperoval and $S_B^\perp$ is a dual hyperoval, all the members S_B^T, $S_B^\perp$, ${S_B}^{T\perp}$, ${S_B}^{\perp T}$ and ${S_B}^{T\perp T}$ are bilinear dual hyperovals. We denote the bilinear mappings which define the above bilinear dual hyperovals by B^T, $B^\perp$, $B^{T\perp}$, $B^{\perp T}$ and $B^{T\perp T}$ respectively. Thus we have $S_B^T = S_{B^T}$, $S_B^\perp = S_{B^\perp}$, ${S_B}^{T\perp} = S_{B^{T\perp}}$, ${S_B}^{\perp T} = S_{B^{\perp T}}$ and ${S_B}^{T\perp T} = S_{B^{T\perp T}}$. Since $B^T(x,t) = t * x$ for $B(x,t) = x * t$, for a Yoshiara's bilinear dual hyperoval S_B with $B(x,t) = x^\sigma t + xt^\tau$, the transpose S_B^T is also a Yoshiara's bilinear dual hyperoval with $B^T(x,t) = x^\tau t + xt^\sigma$. As for an alternating bilinear dual hyperoval S_A, the transpose is $S_A^T = S_A$ since $A^T = A$.

We proved the following theorem in [12].

Theorem 1. *Let f be a quadratic APN function on K. Then, $S_{A_f}^\perp$ is a d-dimensional dual hyperoval in $PG(2d+1,2)$ if, and only if, d is even.*

Hence, if d is even, we have d-dimensional bilinear dual hyperovals $S_{A_f}^\perp = S_{A_f^\perp}$ and $S_{A_f}^{\perp T} = S_{A_f^{\perp T}}$ for any quadratic APN functions f on K by Proposition 7 of [5].

A problem is whether the bilinear dual hyperoval $S_{A_f}^\perp$ or $S_{A_f}^{\perp T}$ belongs to the known families, or not. We will see that $S_{A_f}^\perp$ and $S_{A_f}^{\perp T}$ do not belong to the known families for $f(x) := x^3 + Tr(x^9)$ with $d \geqslant 6$ and d even by proving the following facts: (1) if S_B is isomorphic to some alternating bilinear dual hyperoval S_A, then ϕ_B must be a $GF(2)$-linear mapping (Proposition 3), (2) $\phi_{A_f^\perp}$ and $\phi_{A_f^{\perp T}}$ are not $GF(2)$-linear mapping for $f(x) = x^3 + Tr(x^9)$ (Lemmas 12 and 13), and (3) if $S_{A_f}^\perp$ or $S_{A_f}^{\perp T}$ is isomorphic to some Yoshiara's bilinear dual hyperovals, then f must be extended affine equivalent to a Gold function (Corollaries 5 and 9).

Thus, we prove the following theorem.

Theorem 2. *Let d be even. Let $f(x) := x^3 + Tr(x^9)$ be the quadratic APN function on $K = GF(2^{d+1})$ discovered by Budaghyan, Carlet and Leander in* [2]. *Then, the bilinear dual hyperovals $S_{A_f}^\perp$ and $S_{A_f}^{\perp T}$ are not isomorphic to any bilinear dual hyperoval of Yoshiara or APN type if $d \geqslant 6$.*

It is known that $f(x) := x^3 + Tr(x^9)$ is extended affine equivalent to $g(x) = x^5$ if $d = 4$, and to $g(x) = x^3$ if $d = 5$. (See [6].) Hence S_{A_f} is isomorphic to Yoshiara's bilinear dual hyperoval S_B with $B(x,t) := x^4t + xt^4$ if $d = 4$, and $B(x,t) := x^2t + xt^2$ if $d = 5$ by Theorem 1 of [4]. By Lemma 6 and Example 8, we see that $S^{\perp}_{A_f}$ and $S^{\perp T}_{A_f}$ are isomorphic to Yoshiara's bilinear dual hyperoval S_B with $B(x,t) := x^8t + xt^{16}$ and $B(x,t) := x^{16}t + xt^8$ respectively if $d = 4$. If $d = 5$, $S^{\perp}_{A_f}$ and $S^{\perp T}_{A_f}$ are not a dual hyperovals by Theorem 1.

2. A condition that S_B is isomorphic to some S_A

The isomorphism problem of alternating bilinear dual hyperovals was solved by Edel in [4]. The following proposition will be a step to investigate the isomorphism problem of bilinear dual hyperovals.

Proposition 3. *A bilinear dual hyperoval S_B is isomorphic to some alternating bilinear dual hyperoval S_A if and only if ϕ_B is a $GF(2)$-linear mapping.*

Proof (If part). Assume that ϕ_B is $GF(2)$-linear. Let Φ be a linear automorphism of $K \times K$ defined by

$$\Phi : K \times K \ni (x,z) \mapsto \left(\phi_B^{-1}(x), z\right) \in K \times K.$$

Then, if we put $\phi_B^{-1}(x) := y$, we have

$$\Phi\left(X_B(t)\right) = \left\{\left(\phi_B^{-1}(x), B(x,t)\right) \mid x \in K^{\times}\right\} = \left\{\left(y, B\left(\phi_B(y), t\right)\right) \mid y \in K^{\times}\right\}.$$

Let us set $A(y,t) := B(\phi_B(y), t)$. Since $\phi_B(y)$ is linear by assumption, $A(y,t)$ is bilinear on y and t. It is easy to see that $A(y,t)$ satisfies the conditions (i) and (ii). Moreover, $A(t,t) = B(\phi_B(t), t) = 0$, hence $A(y,t)$ is an alternating mapping. By the mapping Φ, we see that S_B is isomorphic to $S_A := \{X_A(t) \mid t \in K\}$, where $X_A := \{(y, A(y,t)) \mid y \in K^{\times}\}$. □

As for the 'only if part', the proof is easy if an isomorphism from S_B to S_A is given by $\Phi : K \times K \ni (x,y) \mapsto (F(x), H(y)) \in K \times K$ for $GF(2)$-linear mappings F and H. (In this case, Φ fixes the subspace $Y := \{(0,y) \mid y \in K\}$. Then see Definition 3 and Theorem 1 of [4].) However, as in the following proof, we have to assume that $\Phi(x,y) = (F(x) + G(y), H(y))$ using a $GF(2)$-linear mapping G. So, we need a long argument to eliminate G.

Proof (Only if part). Let Φ be a linear mapping which sends S_B to S_A. Since S_A has a translation t_a for $a \in K$ as an automorphism, we may assume that $\Phi(X_B(0)) = X_A(0)$. (Assume that $\Phi(X_B(0)) = X_A(a)$ for some $a \neq 0$. Then if we use $t_a(\Phi((x,y)))$ for $\Phi((x,y))$, we have $t_a(\Phi(X_B(0))) = t_a(X_A(a)) = X_A(0)$.) By assumption, Φ fixes the vector spaces $X_B(0) \cup \{(0,0)\} = X_A(0) \cup \{(0,0)\} = \{(x,0) \mid x \in K\}$. Hence the $GF(2)$-linear mapping Φ is represented as

$$\Phi : K \times K \ni (x,y) \mapsto \left(F(x) + G(y), H(y)\right) \in K \times K$$

where F, G and H are $GF(2)$-linear mappings from K to K. Since Φ is a $GF(2)$-linear automorphism, F and H are $GF(2)$-linear bijections.

Let $A_1(x,t) := H^{-1}(A(F(x), F(t)))$. Then A_1 is an alternating bilinear mapping which also satisfies (i) and (ii). It is easy to see that the dual hyperovals S_A and S_{A_1} are isomorphic by $\Phi' : K \times K \ni (x,y) \mapsto (F^{-1}(x), H^{-1}(y)) \in K \times K$. Now S_B is isomorphic to S_{A_1} by the mapping

$$\Phi_1 : K \times K \ni (x,y) \mapsto \left(x + G_1(y), y\right) \in K \times K,$$

where $G_1(y) = F^{-1}(G(y))$. So without loss of generality, we may assume $A = A_1$, $\Phi = \Phi_1$ and $G = G_1$. From now on, we assume that S_B is isomorphic to S_A by the mapping $\Phi((x, y)) = (x + G(y), y)$.

Since Φ maps every members of S_B onto the members of S_A, there exists a one-to-one mapping $g : K \to K$ such that

$$\Phi : S_B \ni X_B(t) \mapsto X_A\big(g(t)\big) \in S_A$$

for any $t \in K$. Then, since $X_A(g(t)) := \{(y, A(y, g(t))) \mid y \in K^\times\}$, we have

$$\begin{aligned}\Phi : X_B(t) \ni \big(x, B(x,t)\big) &\mapsto \big(x + G\big(B(x,t)\big), B(x,t)\big)\\ &= \big(x + G\big(B(x,t)\big), A\big(x + G\big(B(x,t)\big), g(t)\big)\big) \in X_A\big(g(t)\big).\end{aligned}$$

Hence, for any $x, t \in K$, we see from the second coordinate of $X_A(g(t))$ that

$$B(x,t) = A\big(x + G\big(B(x,t)\big), g(t)\big). \tag{1}$$

Let us substitute x by $\phi_B(t)$. In this proof, we denote $\phi_B(t)$ simply by ϕ. Then, since $B(\phi(t), t) = 0$, we have $A(\phi(t), g(t)) = 0$ by (1). Since $\Phi(X_B(0)) = X_A(0)$, we have $g(0) = 0$. Since g is a one-to-one mapping from K to K, we have $g(t) \neq 0$ if $t \neq 0$. Then, since A is an alternating mapping with the conditions (i) and (ii), we obtain from $A(\phi(t), g(t)) = 0$ that

$$g(t) = \phi(t). \tag{2}$$

Let t_1 and t_2 be elements in K with $t_1 \neq t_2$. If $X_B(t_1) \cap X_B(t_2) \ni (x, B(x, t_1)) = (x, B(x, t_2))$, then $B(x, t_1 + t_2) = 0$, hence we have $x = \phi(t_1 + t_2)$ as $x \neq 0$. If $X_A(\phi(t_1)) \cap X_A(\phi(t_2)) \ni (x, A(x, \phi(t_1))) = (x, A(x, \phi(t_2)))$, then $A(x, \phi(t_1) + \phi(t_2)) = 0$, hence we have $x = \phi(t_1) + \phi(t_2)$ as A is an alternating mapping. Since Φ maps the projective point $X_B(t_1) \cap X_B(t_2)$ to the projective point $X_A(\phi(t_1)) \cap X_A(\phi(t_2))$, we have, for $i = 1, 2$,

$$\Phi\big(\big(\phi(t_1 + t_2), B\big(\phi(t_1 + t_2), t_i\big)\big)\big) = \big(\phi(t_1) + \phi(t_2), A\big(\phi(t_1) + \phi(t_2), \phi(t_i)\big)\big). \tag{3}$$

Since $\Phi((x, y)) = (x + G(y), y)$, we see from the first coordinate of (3) and (2) that

$$\phi(t_1) + \phi(t_2) = \phi(t_1 + t_2) + G\big(B\big(\phi(t_1 + t_2), t_i\big)\big) \tag{4}$$

for $i = 1, 2$. Hence we have

$$\alpha(x,t) := G\big(B\big(\phi(x), t\big)\big) = \phi(x + t) + \phi(x) + \phi(t), \tag{5}$$

which is alternating and linear on t, therefore we see that $\alpha(x, t)$ is an alternating bilinear mapping. In particular, ϕ is quadratic.

Recall the definition of Φ as

$$\Phi\big(\big(x, B(x,t)\big)\big) = \big(x + G\big(B(x,t)\big), B(x,t)\big).$$

Let us substitute x by $\phi(x)$. Then, by (1) and (2), the second coordinate of $\Phi((\phi(x), B(\phi(x), t)))$ is calculated as follows:

$$B\big(\phi(x), t\big) = A\big(\phi(x + t) + \phi(t), \phi(t)\big) = A\big(\phi(x + t), \phi(t)\big). \tag{6}$$

Now, for x and $y \in K$, let $z \in K$ which satisfies that

$$\phi(x) + \phi(y) = \phi(z). \tag{7}$$

We want to prove that $z = x + y$.

Since $B(\phi(x),t)+B(\phi(y),t)=B(\phi(z),t)$ by (7), we obtain from (6) that $A(\phi(x+t)+\phi(t),\phi(t))+A(\phi(y+t)+\phi(t),\phi(t))=A(\phi(z+t)+\phi(t),\phi(t))$, that is,

$$A\big(\phi(x+t)+\phi(y+t)+\phi(z+t)+\phi(t),\phi(t)\big)=0.$$

Since A is an alternating mapping, we have

$$\phi(x+t)+\phi(y+t)+\phi(z+t)=\begin{cases}\phi(t), & \text{or}\\ 0.\end{cases} \tag{8}$$

Since ϕ is a quadratic function, we have

$$\phi(x+y+z)+\phi(x+y)+\phi(y+z)+\phi(z+x)+\phi(x)+\phi(y)+\phi(z)=0 \tag{9}$$

and (if we substitute x by $x+t$, y by $y+t$ and z by $z+t$ in (9), we have)

$$\phi(x+y+z+t)+\phi(x+y)+\phi(y+z)+\phi(z+x)+\phi(x+t)+\phi(y+t)+\phi(z+t)=0. \tag{10}$$

By (7) and (9), we have $\phi(x+y)+\phi(y+z)+\phi(z+x)=\phi(x+y+z)$. Then, by (8) and (10), we have $\phi(x+y+z+t)=\phi(x+y+z)+\phi(t)$ or $\phi(x+y+z+t)=\phi(x+y+z)$. Since ϕ is a one-to-one mapping, for any t, we must have

$$\phi(x+y+z+t)=\phi(x+y+z)+\phi(t).$$

Let $x+y+z:=a$. Then, for any t, we have

$$\phi(a+t)=\phi(a)+\phi(t). \tag{11}$$

If $a=0$ for any x and y, then we have $\phi(x)+\phi(y)=\phi(x+y)$ for any x and y by (7), hence we proved that ϕ is $GF(2)$-linear.

We assume that, there exists $a:=x+y+z\neq 0$ with $\phi(x)+\phi(y)+\phi(z)=0$.

Since $B(\phi(a),t_1)+B(\phi(a),t_2)=B(\phi(a),t_1+t_2)$, by (6), we have

$$\begin{aligned}&A\big(\phi(a+t_1)+\phi(t_1),\phi(t_1)\big)+A\big(\phi(a+t_2)+\phi(t_2),\phi(t_2)\big)\\ &\quad=A\big(\phi(a+t_1+t_2)+\phi(t_1+t_2),\phi(t_1+t_2)\big).\end{aligned}$$

By (11), we have $\phi(a+t_1)+\phi(t_1)=\phi(a)$, $\phi(a+t_2)+\phi(t_2)=\phi(a)$ and $\phi(a+t_1+t_2)+\phi(t_1+t_2)=\phi(a)$ for any t_1 and t_2, hence we have

$$A\big(\phi(a),\phi(t_1)\big)+A\big(\phi(a),\phi(t_2)\big)=A\big(\phi(a),\phi(t_1+t_2)\big),$$

that is,

$$A\big(\phi(a),\phi(t_1)+\phi(t_2)+\phi(t_1+t_2)\big)=0.$$

Since $\phi(a)\neq 0$, for any t_1 and t_2, we have

$$\phi(t_1)+\phi(t_2)=\begin{cases}\phi(t_1+t_2) & \text{or}\\ \phi(t_1+t_2)+\phi(a)=\phi(t_1+t_2+a).\end{cases} \tag{12}$$

(We have $\phi(t_1+t_2)+\phi(a)=\phi(t_1+t_2+a)$ by (11).)

If there exists $a' := x + y + z \neq 0$ for some x, y and z with $\phi(x) + \phi(y) + \phi(z) = 0$ such that $a \neq a'$, and if there exist t_1 and t_2 such that $\phi(t_1) + \phi(t_2) \neq \phi(t_1 + t_2)$, then we obtain from (12) that $\phi(t_1) + \phi(t_2) = \phi(t_1 + t_2) + \phi(a)$ and also we have $\phi(t_1) + \phi(t_2) = \phi(t_1 + t_2) + \phi(a')$ by the same calculation as above, which is a contradiction since $\phi(a) \neq \phi(a')$. Hence, if such an $a \neq 0$ exists, it must be unique.

Now, we assume that there exists such an $a \neq 0$, and assume that there exist t_1 and t_2 such that $\phi(t_1) + \phi(t_2) = \phi(t_1 + t_2) + \phi(a)$.

Since $d + 1 \geqslant 4$, we are able to take $x \in K = GF(2^{d+1})$ which satisfies that

$$x \notin \{0, a, t_1, t_2, t_1 + t_2, t_1 + a, t_2 + a, t_1 + t_2 + a\}. \tag{13}$$

Since $B(\phi(x), t_1) + B(\phi(x), t_2) = B(\phi(x), t_1 + t_2)$, using (6), we have

$$\begin{aligned} &A\big(\phi(x + t_1) + \phi(t_1), \phi(t_1)\big) + A\big(\phi(x + t_2) + \phi(t_2), \phi(t_2)\big) \\ &\quad = A\big(\phi(x + t_1 + t_2) + \phi(t_1 + t_2), \phi(t_1 + t_2)\big). \end{aligned} \tag{14}$$

By (12), there are two possibilities for each value $\phi(x + t_1) + \phi(t_1)$, $\phi(x + t_2) + \phi(t_2)$ and $\phi(x + t_1 + t_2) + \phi(t_1 + t_2)$. That is,

$$\phi(x + t_1) + \phi(t_1) = \begin{cases} \phi(x), & \text{or} \\ \phi(x) + \phi(a), \end{cases}$$

$$\phi(x + t_2) + \phi(t_2) = \begin{cases} \phi(x), & \text{or} \\ \phi(x) + \phi(a), \end{cases}$$

$$\phi(x + t_1 + t_2) + \phi(t_1 + t_2) = \begin{cases} \phi(x), & \text{or} \\ \phi(x) + \phi(a). \end{cases}$$

We have to check the above eight cases to have a contradiction if we assume that $a \neq 0$. However, since we are able to prove all the eight cases in the same way, we only give the proof of the case that $\phi(x + t_1) + \phi(t_1) = \phi(x) + \phi(a)$, $\phi(x + t_2) + \phi(t_2) = \phi(x)$, and $\phi(x + t_1 + t_2) + \phi(t_1 + t_2) = \phi(x) + \phi(a)$ here, and omit the proofs of other cases. In our case, by (14), we have

$$A\big(\phi(x) + \phi(a), \phi(t_1)\big) + A\big(\phi(x), \phi(t_2)\big) = A\big(\phi(x) + \phi(a), \phi(t_1 + t_2)\big).$$

Since A is bilinear, we have

$$A\big(\phi(x), \phi(t_1) + \phi(t_2) + \phi(t_1 + t_2)\big) = A\big(\phi(a), \phi(t_1) + \phi(t_1 + t_2)\big).$$

Since $\phi(t_1) + \phi(t_2) \neq \phi(t_1 + t_2)$ by assumption, we must have $\phi(t_1) + \phi(t_2) = \phi(t_1 + t_2) + \phi(a)$, hence $\phi(t_1) + \phi(t_2) + \phi(t_1 + t_2) = \phi(a)$, that is, $\phi(t_1) + \phi(t_1 + t_2) = \phi(t_2) + \phi(a) = \phi(t_2 + a)$ by (12). From $A(\phi(x), \phi(a)) = A(\phi(a), \phi(t_2 + a))$, we have

$$A\big(\phi(a), \phi(x) + \phi(t_2 + a)\big) = 0.$$

Hence we have $\phi(x) + \phi(t_2 + a) = 0$ or $\phi(a)$. If $\phi(x) + \phi(t_2 + a) = 0$, we have $\phi(x) = \phi(t_2 + a)$, hence $x = t_2 + a$. If $\phi(x) + \phi(t_2 + a) = \phi(a)$, we have $\phi(x) = \phi(t_2 + a) + \phi(a) = \phi(t_2)$ by (11), hence $x = t_2$. In each case, we have a contradiction with the assumption of (13) on x.

Therefore, we conclude that $a := x + y + z = 0$ if $\phi(x) + \phi(y) + \phi(z) = 0$. Thus, we have $\phi(x) + \phi(y) = \phi(x + y)$ for any x and y, that is, ϕ is $GF(2)$-linear. □

Corollary 4. *Let S_B be a Yoshiara's bilinear dual hyperoval with the bilinear form $B(x,t) = x^\sigma t + xt^\tau$, where σ, τ are generators of $Gal(K/GF(2))$ with $\sigma\tau \neq id$. If S_B is isomorphic to some alternating bilinear dual hyperoval S_A, then $\sigma = \tau$.*

Proof. If S_B is isomorphic to some alternating dual hyperoval S_A, then $\phi_B(t) = t^{(\tau-1)/(\sigma-1)}$ must be a $GF(2)$-linear function by Proposition 3. Since $t^{(\tau-1)/(\sigma-1)}$ is a monomial, we have $\phi_B(ab) = \phi_B(a)\phi_B(b)$ for $a, b \in K$ with $\phi_B(0) = 0$ and $\phi_B(1) = 1$. Since $\phi_B(t)$ is a one-to-one mapping from K to K, $\phi_B(t)$ must be an automorphism of K over $GF(2)$. Hence we have $t^{(\tau-1)/(\sigma-1)} = t^\mu$ for some $\mu \in Gal(K/GF(2))$. Let $t^\sigma = t^{2^m}$, $t^\tau = t^{2^n}$ and $t^\mu = t^{2^l}$ for some integers l, m and n with $0 \leqslant l < d+1$ and $0 < m, n < d+1$. Then, we have $t^{(2^n-1)/(2^m-1)} = t^{2^l}$, therefore we have $t^{2^n-1} = t^{2^l(2^m-1)}$. Since $2^{l+m} + 1 \equiv 2^l + 2^n \pmod{2^{d+1}-1}$, we must have $l = 0$, and $m = n$. Thus, we have $\sigma = \tau$. That is, $B(x,t) = x^\sigma t + xt^\sigma$. □

For a generator σ of $Gal(K/GF(2))$, the quadratic APN function $g(x) := x^{\sigma+1}$ is called a Gold function. Using this g, we have an alternating mapping $A_g(x,t) = g(x+t) + g(x) + g(t) + g(0) = (x+t)^{\sigma+1} + x^{\sigma+1} + t^{\sigma+1} = x^\sigma t + xt^\sigma$. Hence, by Corollary 4, if a Yoshiara's bilinear dual hyperoval is isomorphic to some alternating bilinear dual hyperoval, then the Yoshiara's bilinear dual hyperoval must be an APN dual hyperoval S_{A_g} with $g(x) = x^{\sigma+1}$, a Gold function. (We will refer to S_{A_g} as a Gold dual hyperoval.) Thus, we have the following corollary.

Corollary 5. *If an APN dual hyperoval S_{A_f} is isomorphic to some Yoshiara's bilinear dual hyperoval, then f is extended affine equivalent to a gold function $g(x) = x^{\sigma+1}$ for some generator σ of $Gal(K/GF(2))$.*

Proof. Since S_{A_f} is isomorphic to S_{A_g} by Corollary 4, where $g(x) = x^{\sigma+1}$ for some generator σ of $Gal(K/GF(2))$, we see from Theorem 1 of [4] that f is extended affine equivalent to g. □

3. On isomorphisms of the duals of dual hyperovals

We fix a non-degenerate inner product $(\,,\,)$ of $(2d+2)$-dimensional vector space V over $GF(2)$, that is, we fix a non-degenerate symmetric bilinear form over $GF(2)$ from $V \times V$ to $GF(2)$. For a subspace $X \subset PG(2d+1,2) = PG(V) = V\setminus\{\mathbf{0}\}$, let $X^\perp \subset PG(V)$ be the subspace defined by $X^\perp := \{x \mid (x,y) = 0 \text{ for any } y \in X\}$.

Let Φ be a linear automorphism of $PG(V)$. We define the linear automorphism $\Phi^\perp$ of $PG(V)$ as $\Phi^\perp(X^\perp) := \Phi(X)^\perp$ for any subspace $X \subset PG(V)$.

For any d-dimensional subspace $X \subset PG(2d+1,2) = PG(V)$, $X^\perp$ is also a d-dimensional subspace of $PG(V)$. Let S_1 and S_2 be d-dimensional dual hyperovals in $PG(V)$. Since each S_i for $i = 1, 2$ is a collection of d-subspaces of $PG(V)$, we have a collection of d-subspaces $S_i^\perp := \{X^\perp \mid X \in S_i\}$ for $i = 1, 2$.

Now, we assume that $S_1^\perp$ and $S_2^\perp$ are also dual hyperovals, although they are not dual hyperovals in general. (See Theorem 1.) Then, it is easy to see the following lemma and corollary. We omit the proofs since they are consequences of the basic linear algebra.

Lemma 6. *Let S_1 and S_2 be d-dimensional dual hyperovals in $PG(2d+1,2)$. Then a linear automorphism Φ of $PG(2d+1,2)$ induces an isomorphism from S_1 to S_2 if, and only if, $\Phi^\perp$ induces an isomorphism from $S_1^\perp$ to $S_2^\perp$.*

For a d-dimensional dual hyperoval S in $PG(2d+1,2)$, let $Aut(S)$ be the automorphism group of S. Then we have $\Phi \in Aut(S)$ if, and only if, $\Phi^\perp \in Aut(S^\perp)$ by Lemma 6. Hence we have the following corollary.

Corollary 7. *The correspondence $Aut(S) \ni \Phi \mapsto \Phi^\perp \in Aut(S^\perp)$ induces an isomorphism from $Aut(S)$ to $Aut(S^\perp)$.*

4. The duals of some bilinear dual hyperovals

In this section, we determine the duals of the Yoshiara's bilinear dual hyperovals, and of the APN dual hyperoval with quadratic APN function $f(x) = x^3 + Tr(x^9)$ by Budaghyan, Carlet and Leander [2].

Example 8 *(The dual of Yoshiara's bilinear dual hyperoval).* Let σ, τ be generators of $Gal(K/GF(2))$ with $\sigma\tau \neq id$. Let S_B be a Yoshiara's bilinear dual hyperoval with $B(x,t) = x^\sigma t + xt^\tau$. Then, we have $S_B^\perp := \{X_B^\perp(u) \mid u \in K\}$, where

$$X_B^\perp(u) := \left\{ \left(x, x^{\sigma^{-1}}u + xu^{\sigma\tau}\right) \mid x \in K^\times \right\}.$$

If d is even, σ^{-1} and $\sigma\tau$ are both generators of $Gal(K/GF(2))$, hence $S_B^\perp$ is a dual hyperoval in $PG(2d+1,2)$ by Yoshiara [14]. In this case, $S_B^\perp$ is a bilinear dual hyperoval with $B^\perp(x,u) = x^{\sigma^{-1}}u + xu^{\sigma\tau}$.

Proof. $X_B^\perp(t) = \{(x,y) \mid Tr(ys + x(s^\sigma t + st^\tau)) = 0 \text{ for any } s \in K\}$. Now, $Tr(ys + x(s^\sigma t + st^\tau)) = 0$ for any $s \in K$ if and only if $Tr((y + xt^\tau)s + xs^\sigma t) = Tr((y + xt^\tau)s) + Tr(xts^\sigma) = Tr(((y + xt^\tau)^\sigma + xt)s^\sigma) = 0$ for any $s \in K$, since $Tr((y + xt^\tau)s) = Tr((y + xt^\tau)^\sigma s^\sigma)$. By $Tr(((y + xt^\tau)^\sigma + xt)s^\sigma) = 0$ for any $s \in K$, we have $(y + xt^\tau)^\sigma = xt$. Hence, we have $y = x^{\sigma^{-1}}u + xu^{\sigma\tau}$ if we put $u := t^{\sigma^{-1}}$. Therefore, we have $X_B^\perp(u) = \{(x, x^{\sigma^{-1}}u + xu^{\sigma\tau}) \mid x \in K^\times\}$. □

Thus, we see that at least one of $\mathcal{S} := \{S_B, S_B^T, S_B^\perp, S_B^{T\perp}, S_B^{\perp T}, S_B^{T\perp T}\}$ is isomorphic to one of Yoshiara's bilinear dual hyperovals then any element of $\mathcal{S}$ is isomorphic to the Yoshiara's bilinear dual hyperoval if d is even. From Corollary 5, we have the following corollary.

Corollary 9. *Let $\mathcal{S} := \{S_B, S_B^T, S_B^\perp, {S_B}^{T\perp}, {S_B}^{\perp T}, {S_B}^{T\perp T}\}$ and d be even. Let at least one of $\mathcal{S}$ be isomorphic to an APN dual hyperoval. Then S_B is isomorphic to one of Yoshiara's bilinear dual hyperovals if and only if one element of $\mathcal{S}$ is isomorphic to a Gold dual hyperoval.*

Let $f(x) = x^3 + Tr(x^9)$. Then we have $A_f(x,t) := f(x+t) + f(x) + f(t) + f(0) = x^2t + xt^2 + Tr(x^8t + xt^8)$.

Example 10 *($S_{A_f}^\perp$ with the APN function $f(x) = x^3 + Tr(x^9)$).* Let S_{A_f} be an APN dual hyperoval with a quadratic APN function $f(x) = x^3 + Tr(x^9)$, that is, a bilinear dual hyperoval with $A_f(x,t) = x^2t + xt^2 + Tr(x^8t + xt^8)$. Then, we have $S_{A_f}^\perp := \{X_{A_f}^\perp(u) \mid u \in K\}$, where

$$X_{A_f}^\perp(u) := \left\{ \left(x, xu^4 + x^2u^{16} + Tr(x)\left(u + u^{64}\right)\right) \mid x \in K^\times \right\}.$$

If d is even, then $S_{A_f}^\perp$ is a dual hyperoval in $PG(2d+1,2)$ by Theorem 1, hence $S_{A_f}^\perp$ is a bilinear dual hyperoval with $A_f^\perp(x,u) = xu^4 + x^2u^{16} + Tr(x)(u + u^{64})$.

Proof. Let us denote x^8 by x^τ. Then, the equation $Tr(ys + x(s^2t + st^2 + Tr(s^\tau t + st^\tau))) = 0$ is also expressed as

$$Tr\left(ys + x\left(s^2t + st^2 + \sum_{\sigma \in Gal(K/GF(2))} \left(s^\tau t + st^\tau\right)^\sigma\right)\right) = 0.$$

Using this expression, we have $Tr(ys + x(s^2t + st^2 + Tr(s^\tau t + st^\tau))) = 0$ for any $s \in K$ if, and only if,

$$
\begin{aligned}
&Tr\Big(\big(y+xt^2\big)s+xts^2+x\sum_{\sigma\in Gal(K/GF(2))}\big(s^{\sigma\tau}t^{\sigma}+s^{\sigma}t^{\sigma\tau}\big)\Big)\\
&=Tr\big(\big(y+xt^2\big)s\big)+Tr\big(xts^2\big)+\sum_{\sigma\in Gal(K/GF(2))}\big(Tr\big(xs^{\sigma\tau}t^{\sigma}\big)+Tr\big(xs^{\sigma}t^{\sigma\tau}\big)\big)\\
&=Tr\big(\big(y+xt^2\big)s\big)+Tr\big((xt)^{2^{-1}}s\big)+\sum_{\sigma\in Gal(K/GF(2))}\big(Tr\big(x^{(\sigma\tau)^{-1}}t^{\tau^{-1}}s\big)+Tr\big(x^{\sigma^{-1}}t^{\tau}s\big)\big)\\
&=Tr\Big(\Big(\big(y+xt^2\big)+x^{2^{-1}}t^{2^{-1}}+\sum_{\sigma\in Gal(K/GF(2))}\big(x^{\sigma^{-1}\tau^{-1}}t^{\tau^{-1}}+x^{\sigma^{-1}}t^{\tau}\big)\Big)s\Big)\\
&=Tr\big(\big(\big(y+xt^2\big)+x^{2^{-1}}t^{2^{-1}}+Tr(x)t^{\tau^{-1}}+Tr(x)t^{\tau}\big)s\big)=0
\end{aligned}
$$

for any $s\in K$. Recall the fact that, for $\alpha\in K$, if $Tr(\alpha s)=0$ for any $s\in K$, then α must be 0. Hence, from $Tr(((y+xt^2)+x^{2^{-1}}t^{2^{-1}}+Tr(x)t^{\tau^{-1}}+Tr(x)t^{\tau})s)=0$ for any $s\in K$, we have $(y+xt^2)+x^{2^{-1}}t^{2^{-1}}+Tr(x)t^{\tau^{-1}}+Tr(x)t^{\tau}=0$, hence

$$y=xt^2+x^{2^{-1}}t^{2^{-1}}+Tr(x)t^{8^{-1}}+Tr(x)t^8.$$

Now, let us put $x':=x^{2^{-1}}$ and $u:=t^{8^{-1}}$, then since $x=(x')^2$, $t^{2^{-1}}=u^4$, $t^2=u^{16}$ and $t^8=u^{64}$, we have

$$y=x'u^4+\big(x'\big)^2u^{16}+Tr\big(x'\big)\big(u+u^{64}\big).$$

Thus $S^{\perp}_{A_f}$ is a bilinear dual hyperoval with $A^{\perp}_f(x',u)=x'u^4+(x')^2u^{16}+Tr(x')(u+u^{64})$. □

By Example 10, we have a bilinear dual hyperoval S_B with

$$B(x,t)=xt^4+x^2t^{16}+Tr(x)\big(t+t^{64}\big)$$

if d is even. We note that the dual $S^{\perp}_B$ is isomorphic to the APN dual hyperoval S_{A_f} with a quadratic APN function $f(x)=x^3+Tr(x^9)$ by Lemma 6.

Example 11 *($S^{\perp T}_{A_f}$ with $f(x)=x^3+Tr(x^9)$).* Let d be even. Then, since $S^{\perp}_{A_f}$ with $A^{\perp}_f(x,t)=xt^4+x^2t^{16}+Tr(x)(t+t^{64})$ is a bilinear dual hyperoval as in Example 10, we see that the transpose $S^{\perp T}_{A_f}$ with $A^{\perp T}_f(x,t)=x^4t+x^{16}t^4+Tr(t)(x+x^{64})$ is also a bilinear dual hyperoval.

In the following Lemma 12 and Corollary 14, we prove that S_B and S^T_B for $B(x,t):=A^{\perp}_f(x,t)$ and $B^T(x,t):=A^{\perp T}_f(x,t)$ are not isomorphic to any APN dual hyperoval.

Lemma 12. *Let d be even. Then d-dimensional bilinear dual hyperoval S_B with $B(x,t):=xt^4+x^2t^{16}+Tr(x)(t+t^{64})$ is not isomorphic to any alternating bilinear dual hyperoval.*

Proof. Let us consider the function $\phi_B:K\to K$ with $B(\phi_B(t),t)=0$ of Proposition 3, where

$$B(x,t):=xt^4+x^2t^{16}+Tr(x)\big(t+t^{64}\big).$$

We assume that the dual hyperoval S_B is isomorphic to some alternating dual hyperoval S_A to have a contradiction. By Proposition 3, we assume that ϕ_B is $GF(2)$-linear.

Let $H := \{x \in K \mid Tr(x) = 0\}$. Let $x \in H$ with $x \neq 0$. Then from $B(x,t) = 0$ with $t \neq 0$, we have $x = \phi_B(t) = 1/t^{12}$. Indeed, since $Tr(x) = 0$, we have $B(x,t) = xt^4 + x^2t^{16} = 0$, hence we have $x = 1/t^{12}$.

Since $t_1 + t_2 \in H$ for $t_1, t_2 \in H$, and since ϕ_B is $GF(2)$-linear by assumption, we have

$$1/t_1^{12} + 1/t_2^{12} = \phi_B(t_1) + \phi_B(t_2) = \phi_B(t_1 + t_2) = 1/(t_1 + t_2)^{12}.$$

However, from $1/t_1^{12} + 1/t_2^{12} = 1/(t_1 + t_2)^{12}$ with $t_1 \neq t_2$, we easily see $t_1^7 + t_2^7 = (t_1 + t_2)(t_1^6 + t_1^5t_2 + t_1^4t_2^2 + t_1^3t_2^3 + t_1^2t_2^4 + t_1t_2^5 + t_2^6) = 0$, hence we have $t_1^7 = t_2^7$. Then, since $(t_2/t_1)^7 = 1$ for any non-zero $t_1, t_2 \in \phi_B^{-1}(H)$, we have $\{t_2/t_1 \mid t_2 \in \phi_B^{-1}(H)\} \subset GF(2^3)$ for some non-zero $t_1 \in \phi_B^{-1}(H)$. Since the cardinality $|K| = 2^{d+1}$ with $d \geqslant 3$, we have $|H| = |\phi_B^{-1}(H)| \geqslant 8$. Hence, we must have $d = 3$, which contradicts our assumption that d is even. Therefore, we conclude that ϕ_B is not $GF(2)$-linear. By Proposition 3, we see that S_B is not isomorphic to any alternating bilinear dual hyperoval. □

Lemma 13. *A bilinear dual hyperoval S_B is not isomorphic to any alternating bilinear dual hyperoval if and only if the transpose S_B^T is not isomorphic to any alternating bilinear dual hyperoval.*

Proof. Let ϕ_{B^T} be a bijective mapping from K to itself which satisfies that $B^T(\phi_{B^T}(t), t) = 0$ for all $t \in K$. Since $B^T(x,y) = B(y,x)$, it follows from $B^T(\phi_{B^T}(t), t) = B(t, \phi_{B^T}(t)) = 0$ for all $t \in K$ that $\phi_{B^T} = \phi_B^{-1}$. Hence, ϕ_B is a $GF(2)$-linear bijection if and only if ϕ_{B^T} is a $GF(2)$-linear bijection. Therefore, we see that S_B is not isomorphic to any alternating bilinear dual hyperoval if and only if S_B^T is not isomorphic to any alternating bilinear dual hyperoval by Proposition 3. □

Corollary 14. *Let d be even. Then, d-dimensional bilinear dual hyperoval $S_B^T = S_{B^T}$ with $B^T(x,t) := x^4t + x^{16}t^2 + Tr(t)(x + x^{64})$ is not isomorphic to any alternating dual hyperoval.*

5. Proof of Theorem 2

We have to prove that, for $f(x) = x^3 + Tr(x^9)$, the bilinear dual hyperovals $S_{A_f^\perp} := S_{A_f}^\perp$ and $S_{A_f^{\perp T}} := S_{A_f}^{\perp T}$ are not isomorphic to an APN dual hyperovals and to Yoshiara's bilinear dual hyperovals for $d \geqslant 6$, where $A_f^\perp(x,t) = xt^4 + x^2t^{16} + Tr(x)(t + t^{64})$ and $A_f^{\perp T}(x,t) := x^4t + x^{16}t^2 + Tr(t)(x + x^{64})$. (See Examples 10 and 11.) Indeed, $S_{A_f^\perp}$ and $S_{A_f^{\perp T}}$ are not isomorphic to any APN dual hyperoval by Lemma 12 and Corollary 14, and $S_{A_f^\perp}$ and $S_{A_f^{\perp T}}$ are not isomorphic to any Yoshiara's bilinear dual hyperoval by Corollary 9, since the APN function $f(x) = x^3 + Tr(x^9)$ is CCZ inequivalent, hence extended affine inequivalent, to a Gold function for $d \geqslant 6$. (See Theorem 3 and Corollary 3 of Budaghyan, Carlet and Leander [2].) □

Acknowledgments

The author would like to express his thanks to Y. Edel for his kind advices. The author also express his thanks to the referees for their helpful comments.

References

[1] S. Ball, M.R. Brown, The six semifield plane associated with a semifield flock, Adv. Math. 189 (2004) 68–87.
[2] L. Budaghyan, C. Carlet, G. Leander, Constructing new APN functions from known ones, Finite Fields Appl. 15 (2009) 150–159.
[3] A. Del Fra, On d-dimensional dual hyperovals, Geom. Dedicata 79 (2000) 157–178.
[4] Y. Edel, On quadratic APN functions and dimensional dual hyperovals, Des. Codes Cryptogr. 57 (1) (2010) 35–44.
[5] Y. Edel, On some representations of quadratic APN functions and dimensional dual hyperovals, RIMS Kokyuroku 1687 (2010) 118–130.
[6] Y. Edel, Personal communication, February, 2010.
[7] C. Huybrechts, A. Pasini, Frag transitive extensions of dual affine spaces, Beitrage Algebra Geom. 40 (1999) 503–532.

[8] D.E. Knuth, Finite semifields and projective planes, J. Algebra 2 (1965) 182–217.
[9] F. Göloğlu, A. Pott, Almost perfect nonlinear functions: A possible geometric approach, in: S. Nicova, B. Preneel, L. Storme, J.A. Thas (Eds.), Proceedings of the Contact Forum Coding Theory and Cryptography 2, The Royal Fremish Academy of Belgium for Science and Arts, 2007, pp. 75–100.
[10] H. Taniguchi, On a family of dual hyperovals over $GF(q)$ with q even, European J. Combin. 26 (2005) 195–199.
[11] H. Taniguchi, On an isomorphism problem of some dual hyperovals in $PG(2d+1,q)$ with q even, Graphs Combin. 23 (2007) 455–465.
[12] H. Taniguchi, On the duals of some dual hyperovals in $PG(2d+1,2)$, Finite Fields Appl. 15 (2009) 673–681.
[13] H. Taniguchi, S. Yoshiara, On dimensional dual hyperovals $S^{d+1}_{\sigma,\phi}$, Innov. Incidence Geom. 1 (2005) 197–219.
[14] S. Yoshiara, A family of d-dimensional dual hyperovals in $PG(2d+1,2)$, European J. Combin. 20 (1999) 589–603.
[15] S. Yoshiara, Dimensional dual hyperovals associated with quadratic APN functions, Innov. Incidence Geom. 8 (2009).
[16] S. Yoshiara, Notes on APN functions, semibiplanes and dimensional dual hyperovals, Des. Codes Cryptogr. 56 (2010) 197–218.